# R E M A R K S

In the Office Action, the Examiner rejected the claims under 35 USC §102.  The claims have been amended to further clarify the subject matter regarded as the invention.  The rejections are fully traversed below.  Claims 1-4, 6-31, and 33-55 remain pending.

Reconsideration of the application is respectfully requested based on the following remarks.

## REJECTION OF CLAIMS UNDER 35 USC §102

In the Office Action, the Examiner has rejected claims 1-4, 6-31, and 33-55 under 35 USC §102(e) as being anticipated by Malinen et al, U.S. Patent Pub. No. 2003/0028763, ('Malinen' hereinafter).  This rejection is fully traversed below.

Claim 1, as amended, is directed to a method performed by a server.  Claim 1 recites, in part:

receiving a request message <u>by the server</u> from a Home Agent, the request message identifying the Mobile Node;

deriving key information <u>by the server</u> from a key or password associated with the Mobile Node; and

sending a reply message <u>by the server</u> to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information;

wherein the reply message does not include the shared key to be shared between the Mobile Node and the Home Agent in any form.

Malinen fails to disclose or suggest "receiving a request message <u>by the server</u> from a Home Agent, the request message identifying the Mobile Node."  The Examiner refers to FIG. 2, step 215.  However, this step shows a Mobile Node sending a message, not a Home

Agent. In other words, a request message is not received from a Home Agent. It is unclear which device the Examiner is interpreting as a Home Agent.

It is also important to note that the steps disclosed in Malinen as cited by the Examiner are not all performed by a server that is adapted for performing authentication, authorization, and accounting. Rather, the steps of Malinen referred to by the Examiner are performed by various different devices as set forth in Malinen. For instance, step 215 shows that an AR/LA receives a message from a Mobile Node (rather than a server that is adapted for performing authentication, authorization, and accounting), while steps 230-240 of Malinen are initiated by a AGW/AAAH.

Even if the AR/LA of Malinen is interpreted to be a Home Agent, a session key is actually transmitted to the AR/LA of Malinen. More specifically, paragraph 185 discloses that "the local attendant will receive a key reply (275) with a success status and potentially with the generated session key." There is no indication that the server sends a reply message to a Home Agent, where the reply message includes key information that enables the Home Agent to derive a shared key from the key information. In fact, there is no disclosure in Malinen indicating that a Home Agent can derive a shared key that is shared between the Mobile Node and the Home Agent. Accordingly, Applicant respectfully asserts that Malinen fails to anticipate claim 1.


Claim 10, as amended, is directed to a method performed by a Home Agent. Claim 10 recites, in part:

receiving a Mobile IP registration request by the Home Agent from a Mobile Node, the Mobile IP registration request identifying the Mobile Node;

sending a request message by the Home Agent to a AAA server, the request message identifying the Mobile Node;

receiving a reply message by the Home Agent from the AAA server, the reply message including key information associated with the Mobile Node;

deriving a key by the Home Agent from the key information, the key being a shared key between the Mobile Node and the Home Agent, wherein deriving the key from the key information does not include decryption of the key information; and

sending a Mobile IP registration reply by the Home Agent to the Mobile Node, wherein the Mobile IP registration reply does not include the key in any form.

As recited in claim 10, the Home Agent derives the key, where the key is a shared key between the Mobile Node and the Home Agent. This derivation is initiated upon receipt of a Mobile IP registration request from the Mobile Node.

Malinen fails to disclose "receiving a Mobile IP registration request <u>by the Home Agent</u> from a Mobile Node, the Mobile IP registration request identifying the Mobile Node." The Eaminer cites step 215. However, Malinen clearly discloses that this message is a AAAv6 request, and makes no mention of a Mobile IP registration request.
With respect to the limitation, "sending a request message <u>by the Home Agent</u> to a AAA server, the request message identifying the Mobile Node." The Examiner cites step 225, which appears to indicate that the Examiner is interpreting AAAL to be the Home Agent. Thus, Malinen fails to disclose or suggest "receiving a reply message <u>by the Home Agent</u> from the AAA server, the reply message including key information associated with the Mobile Node." More specifically, the Examiner cites paragraph [0180]. However, paragraph [0180] merely refers to step 215 of FIG. 2. As set forth above, step 215 discloses a Mobile Node sending a message to AR/LA. Thus, here, it appears that the Examiner may be interpreting the AR/LA to be the Home Agent – which is inconsistent with the above rejection (which implies that the Examiner is interpreting AAAL to be the Home Agent). Moreover, step 215 clearly indicates that the sender of this message is the Mobile Node, and not a AAA server.

In addition, Malinen fails to disclose "deriving a key <u>by the Home Agent</u> from the key information, the key being a shared key between the Mobile Node and the Home Agent, wherein deriving the key from the key information does not include decryption of the key information." In fact, as set forth above, paragraph 185 discloses that "the local attendant will receive a key reply (275) with a success status and potentially with the generated session key." Thus, the session key is received by the LA. There is no indication that an entity that could be interpreted as a Home Agent derives a session key.

Moreover, Malinen fails to disclose or suggest, "sending a Mobile IP registration reply <u>by the Home Agent</u> to the Mobile Node, wherein the Mobile IP registration reply does not include the key in any form." The Examiner cites step 245, which merely discloses that a Mobile Node sends a AAA message to AR/LA. Thus, this message is not a Mobile IP registration reply, and is not sent by a Home Agent. Accordingly, Applicant respectfully asserts that Malinen fails to anticipate claim 10.

Claim 36 is directed to a method performed by a Mobile Node. Claim 36 recites, in part:

sending a <u>Mobile IP</u> registration request <u>from the Mobile Node</u> to the Home Agent;

receiving a <u>Mobile IP</u> registration reply <u>by the Mobile Node</u> from the Home Agent, the <u>Mobile IP</u> registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent, wherein the Mobile IP registration reply does not include the key to be shared between the Mobile Node and the Home Agent in any form; and

deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node, wherein deriving the key from the key information does not include decryption of the key information.

As set forth above, Malinen says nothing about the sending of Mobile IP registration request or registration reply messages in the manner claimed. Accordingly, Applicant respectfully asserts that claim 36 is patentable over Malinen.

The additional limitations recited in the independent claims or the dependent claims are not further discussed, as the above discussed limitations are clearly sufficient to distinguish the claimed invention from the cited reference. Thus, it is respectfully requested that the Examiner withdraw the rejection of the claims under 35 USC §102.

## SUMMARY

If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 504480 (Order No. CISCP334).

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Elise R. Heilbrunn/
Elise R. Heilbrunn
Reg. No. 42,649

P.O. Box 70250
Oakland, CA 94612-0250
Tel: (510) 663-1100